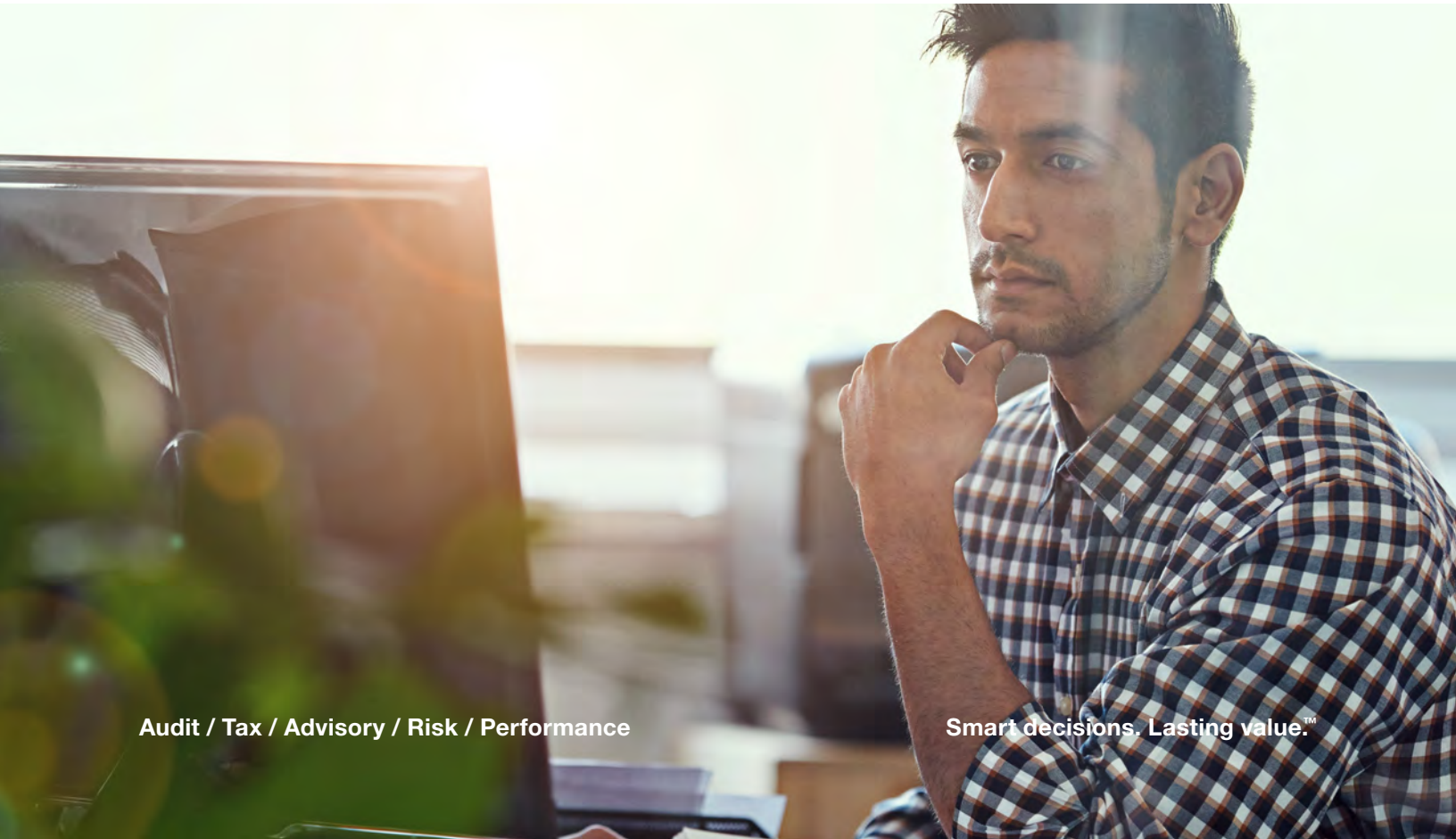
November 2018

Protecting Personal and Sensitive Data Entrusted to Third Parties

An article by Mindy R. Herman and Michael L. Lucas



Protecting personal and company confidential data that they collect, process, or store should be a top priority for organizations. Failure to comply with data protection regulations and leading practices has potentially devastating consequences, including financial penalties, reputational damage, decreased consumer loyalty, and loss of business value.

Increasing regulatory requirements related to personal data protection underscore these risks. Notably, effective May 25, 2018, companies that access or process information about European Union subjects need to comply with the General Data Protection Regulation (GDPR), which requires companies to meet strict provisions and respect individuals' choices regarding handling of their personal data. This and an array of other regulatory requirements will demand companies stay vigilant regarding data protection.

Compliance efforts for protecting sensitive information can seem all-consuming to companies, especially in the face of new regulations. However, if they act strategically, companies that work to mature and refine their privacy and data protection programs will benefit in the long term by being better positioned to protect *all* their data, including valuable intellectual property, company confidential information, and personal data. As part of their compliance efforts, companies must be responsible for information entrusted to third parties as well. Following are some data protection expectations that will support compliance obligations and protect business value when companies rely on third parties.

Data protection expectations for third parties

To remain competitive, innovative, and scalable, organizations often engage with third parties for expertise and specialized solutions. This results in a company's most sensitive data – including personal data and intellectual property – being stored and processed by those third parties during the course of business.

Organizations working with third parties should have data protection expectations for those businesses, including knowing what controls are in place at the third party to help protect information. Some data protection considerations pertaining to a relationship with third parties include the following categories of controls:

- **People controls**
  - Training and awareness
  - Background checks
  - Data ownership and governance
- **Technology controls**
  - Data loss prevention monitoring
  - Encryption
  - Data transfer mechanism
  - Data destruction
  - Network security
- **Process controls**
  - Data classification
  - Network and platform management
  - User and privilege management
  - Data inventory
  - Lawful processing
  - Privacy notice and consent
  - Breach notification time frames
  - Data subject rights procedures
  - System development life cycle methodology
  - Data protection impact assessment

Companies should validate the effectiveness of these controls by considering data protection issues during each phase of a typical third-party relationship life cycle:

Phase 1: Planning and strategy. Before entering a contract with a third party, organizational leadership should consider all possible associated risks and what needs to be done to manage those risks.

Phase 2: Due diligence. If the risks identified during phase one are high, an organization should perform due diligence to validate that appropriate people, processes, and technology controls are in place and are effective. Some approaches to validating controls include:

- Independent attestations, such as reviewing System and Organization Controls reports and certifications
- Technical evaluations, such as penetration testing
- Structured questionnaires asking the third party to share details about its controls
- Evidence-based assessments in which assessors meet on-site or remotely with the third-party processor to validate that controls are in place
- Internal audit of the third party, with detailed testing of controls

Phase 3: Contracting. In the contract phase, an organization has an opportunity to word the contract to begin managing data protection risks. For example, an organization might include structured language about how the third-party vendor will protect sensitive data.

Phase 4: Ongoing management. Once a contract is signed and the relationship with the third party proceeds, an organization should implement ongoing monitoring of third-party operation. Examples include monitoring for reported data breaches and obtaining attestation and penetration assessment reports as they become available.

Phase 5: Periodic re-evaluation. Even if due diligence has been conducted in the earlier stages of a partnership, it's wise to intermittently re-evaluate the third party with the same level of scrutiny as during initial due diligence.

Aligning internal and external data protection efforts

To help identify their data protection expectations for external partners, companies should look to their own documented IT and security controls and standards such as password and internet use policies and human resource policies regarding background checks. Companies should have these same security expectations for third parties that will have access to personal data.

Working as a team

An effective data protection program – especially one that extends to third parties – cannot be managed in isolation. It needs to be a team effort, involving stakeholders from multiple areas across the organization, including:

- Procurement, for sourcing and contracting
- IT, to establish and maintain security standards and devise a framework for standards expected of external partners
- Legal, to assist with contracting and compliance issues, including those related to privacy laws
- An overall third-party risk management function, to bring all the other departments together and oversee data protection activity

An ongoing effort

Protecting critical data and remaining compliant with data security regulations is an ongoing endeavor for most organizations. Companies should use their work toward regulatory compliance as an opportunity to improve all aspects of data protection. Continually working to enhance their privacy and data protection programs will help businesses stay compliant and prepared for whatever new regulations may be ahead.

Learn more

Mindy Herman
Principal
+1 317 706 2614
mindy.herman@crowe.com

Michael Lucas
+1 312 632 6560
michael.lucas@crowe.com

crowe.com

MD-19001-012A